PJG.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/306,110	05/06/1999	SATOSHI HASEGAWA	P/2850-19	3039

7590 07/30/2003

Dicksein Shapiro Morin & Oshinsky LLP
1177 Avenue of the Americas
NEW YORK, NY 10036-2714

EXAMINER	
VAUGHAN, MICHAEL R	
ART UNIT	PAPER NUMBER
2131	6

DATE MAILED: 07/30/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

PR4

Office Action Summary	**Application No.** 09/306,110	**Applicant(s)** HASEGAWA, SATOSHI	
	Examiner Michael R Vaughan	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)□ Responsive to communication(s) filed on _____ .

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)□ Claim(s) _____ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-14 is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 06 May 1999 is/are: a)□ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)□ The proposed drawing correction filed on _____ is: a)□ approved b)□ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)□ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.☒ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____ .

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)□ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) □ The translation of the foreign language provisional application has been received.

15)□ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☒ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 4 .

4) □ Interview Summary (PTO-413) Paper No(s). _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: .

Detailed Actions

Claims 1-14 have been examined.

Drawings

The drawings are objected to because FIG. 3, reference B3 has the word "cord". This should be change to –code--. A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Specification

The disclosure is objected to because of the following informalities: inconsistent naming to reference 7 in FIG. 1. On page 5, line 21, reference number 7 is referred to as "variation creation unit". On page 6, line 19, reference number 7 is referred to as "variable creation unit". Reference 7 should be only referred to by one entity. The applicant should carefully review the rest of the application for other inconsistencies. Sentence starting on page 11, line 10 needs further proof reading.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 3, 5, 8, 9, are rejected under 35 U.S.C. 103(a) as being unpatentable over Hűtter (USP 6,160,785) in view of Becker (USP 4,157,454).

As per claim 1, Hűtter teaches a data transmission system comprising:

a stream buffer (column 4, lines 11-12);

stream processing means (column 4, 22-23);

output means (column 4, 22-23). Hűtter's art teaches the process of reading from a digital stored medium, to place that data into a buffer until it can be processed, and then outputted. Hűtter is silent in disclosing a means to perform calculations, inverse calculations, and creating variables.

Becker teaches:

enciphering (calculating) data using a key or keys (variable) (column 18, lines 36-40);

deciphering (inverse calculating) (column 18, lines 55-58);

enciphering key generation (variable creation means) (column 2, lines 60-66).

Becker also discloses that it is well known to provide enciphering systems at those points of the system which are particularly liable to unauthorized access (column 1, lines 13-18). One such liable point is memory. It is well known in the art that reading memory (a place for temporarily storing data) is a fundamental computer process. Therefore it would be obvious to one in the art that if you want to protect memory from being read you should encipher it. Becker's cipher method is one way to protect memory. In view of this, it would have been obvious to one in the art at the time of this invention to use an enciphering method to protect the buffer (memory) of Hűtter's data transmission system.

As per claim 3, Becker teaches that one can implement a programmable logic array, PLA, which is known in the art, to cause random changes in the enciphering keys (column 17, lines 51-56). This would add increased safety. In view of this, it would have been obvious to one of ordinary skill in the art at the time of the invention to change the variables (keys) at arbitrary times. Clearly the motivation is to increase the overall security of the calculation means.

As per claim 5, Hűtter is silent in disclosing creating multiple keys. Becker teaches creating a number of keys (column 3, lines 1-13). Having multiple keys gives the calculator choice as to which variable (key) to use in calculating the input data. This choice further increases the security of the system. In view of this, it would have been obvious to one of ordinary skill in the art at the time of the invention to create multiple variables (keys).

As per claim 8, the examiner supplies the same rationale for the motivation as recited in rejection of claim 1. In addition, Hűtter is silent in disclosing a means for creating multiple keys.

Becker teaches creating a number of keys (column 3, lines 1-13). Having multiple keys gives the calculator choice as to which variable (key) to use in calculating the input data. This choice further increases the security of the system. In view of this, it would have been obvious to one of ordinary skill in the art at the time of the invention to create multiple variables (keys). Furthermore, Hűtter is silent in disclosing modification modes. Becker teaches that modification modes (variable change codes) result in the changing of keys (variables) (column 2, lines 53-55). Modification modes are signals to let the system know when a change of keys (variables) is taking place. Sending a modification mode signals that a change in keys has occurred. The absence of a modification mode signifies to continue to use the current key. This is a necessary function because the inverse calculator would not know when to use its new variable to decipher future data. The inverse calculator needs to know which variable to use to successfully decipher the data. In view of this, it would have been obvious to one of ordinary skill in the art at the time of the invention to use variable change codes to notify the inverse calculator of a change in variables.

As per claim 9, Hűtter is silent in disclosing a changing the variable after each cycle. Becker teaches changing the variable after each enciphering operation (cycle) (column 2, lines 53-55). Clearly the motivation is to increase the overall security of the system. Changing the variable after each cycle greatly increases the work necessary to one trying to compromise the system. The more ways you encipher data, the more ways one has to decipher them. In view of this, it would have been obvious to one of ordinary skill in the art at the time of the invention to change variables after each enciphering cycle to make the system more resistant to unauthorized deciphering.

As per claim 10, the examiner supplies the same rationale for the motivation as recited in rejection of claim 3.

Claims 2 and 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hűtter and Becker as applied to claims 1 and 5 above, and further in view of Hanson (USP 5,132,955).

As per claim 2, the combination of Hűtter and Becker are silent in disclosing the amount of data read into the buffer. Hanson's clearly suggests that buffer overflows should be prevented.

He teaches that adjusting the speed of the CD can prevent buffer overflow (column 5, lines 19-23). Knowing at what rate to read data is directly proportional to the rate at which the data can be processed. If more data is read into the buffer than the processor can handle, a buffer overflow will occur. This is notoriously known in the art. In view of this, it would have been obvious to one of ordinary skill in the art at the time of the invention to input only an amount of data, which can be processed at a time.

As per claim 6, the examiner supplies the same rationale for the motivation as recited in rejection of claim 2.

Claims 4, 7, 11-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hűtter and Becker as applied to claims 1-3, 5, 6, and 10 above, and further in view of Kato et al (US Patent Application 10/035,311).

As per claim 4, Hűtter and Becker are silent in disclosing how the deciphering means (inverse calculator) obtain new deciphering keys (variable change codes). Kato teaching the use of a master key and session keys to notify the deciphering means when the enciphering means (calculator) has changed keys (variable change code) (page 7, paragraphs 0110-0111). The enciphering means sends a new session key to the deciphering means, which it uses to decipher future data. It is obvious that the deciphering means needs to know how the data it is receiving has been enciphered, in order to correctly decipher it. Kato teaches how this can be done. In view of this, it would have been obvious to one of ordinary skill in the art at the time of the invention to pass a variable change code from the calculator to the inverse calculator. In the context of this invention, it is obvious that the code must travel from the calculator to the inverse calculator via the buffer because that is the only data path to connecting the two.

As per claims 7, 11-14, the examiner supplies the same rationale for the motivation as recited in rejection of claim 4.

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Brown et al, U.S. Patent 3,715,489

Atalla, U.S. Patent 4,268,715

Chen et al, U.S. Patent 5,917,830

Yanovsky, U.S. Patent 5,703,948

Takeuchi et al, JP402087199 A

Kotoda, JP409128475 A

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael R Vaughan whose telephone number is 703-305-0354. The examiner can normally be reached on M-F 7-3:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone numbers for the organization where this application or proceeding is assigned are 703-746-7239 for regular communications and 703-746-7239 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Michael R Vaughan
Examiner
Art Unit 2131

MV

July 28, 2003

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100